On the Density of the Set of Known Hadamard Orders

Warwick de Launey and Daniel M. Gordon[*]

April 28, 2010

Abstract

Let $S(x)$ be the number of $n \leq x$ for which a Hadamard matrix of order n exists. Hadamard's conjecture states that $S(x)$ is about $x/4$. From Paley's constructions of Hadamard matrices, we have that

$$S(x) = \Omega\left(\frac{x}{\log x}\right).$$

In a recent paper, the first author suggested that counting the products of orders of Paley matrices would result in a greater density. In this paper we use results of Kevin Ford to show that it does:

$$S(x) \geq \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right),$$

where $C = 0.8178\ldots$.

This bound is surprisingly hard to improve upon. We show that taking into account all the other major known construction methods for Hadamard matrices does not shift the bound. Our arguments use the notion of a (multiplicative) monoid of natural numbers. We prove some initial results concerning these objects. Our techniques may be useful when assessing the status of other existence questions in design theory.

[*] The authors are with the IDA Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121 USA (email: {warwick,gordon}@ccrwest.org).

1 Introduction

In this paper we use the idea of the density of a set of natural numbers $\mathbb{N}$ to gauge the progress made so far on the Hadamard Conjecture. In addition, we propose that our methodology could be used to assess the status of other existence problems in design theory.

We take a moment to describe some ideas concerning (infinite) subsets of $\mathbb{N}$, their sizes and their densities. Section 2 covers these and related ideas in more detail. Given a set $\mathcal{A}$ of positive integers, we may define a *counting function* $A : \mathbb{R} \to \mathbb{N}$, where $A(x) = \#\{n \leq x \mid n \in \mathcal{A}\}$. The rate of growth of this function is used by number theorists to gauge the size of the set $\mathcal{A}$. For example, the counting function $\pi(x)$ of the set of primes is approximately equal to $x/\log x$.

In this paper, sets will be in calligraphic font, and the counting function for a set will be the same letter in roman font. We will respectively call the function $A(x)$, and the ratio function $A(x)/x$ the *size* and *density* (functions) of the set $\mathcal{A}$. So the set of odd natural numbers has size about $x/2$ and density about $1/2$.

Hadamard's conjecture states:

Conjecture 1.1. *For every odd number k there is a Hadamard matrix of order $2^s k$ for $s \geq 2$.*

Let $\mathcal{S}$ be the set of orders for which a Hadamard matrix exists, and let $S(x)$ be the size function of $\mathcal{S}$. Then, since there are also Hadamard matrices of orders 1 and 2, Conjecture 1.1 is equivalent to:

Conjecture 1.2. *For every $x \geq 2$,*

$$S(x) = \left\lfloor \frac{x}{4} \right\rfloor + 2\,.$$

There are a number of existence theorems for Hadamard matrices, but we are far from being able to prove Conjecture 1.2. The conjecture implies that the set $\mathcal{S}$ of Hadamard orders has density $1/4$. As yet, we have not even been able to prove that $\mathcal{S}$ has positive density. In this paper we derive lower bounds for $S(x)$ using known existence theorems. Using Paley's constructions we immediately get a density of $O(x/\log x)$. Using results on the density of values of Euler's totient function we show:

Theorem 1.3. *For all $\epsilon > 0$, there is an element $x_\epsilon \in \mathbb{N}$ such that, for all $x > x_\epsilon$,*

$$S(x) \geq \frac{x}{\log x} \exp\left((C+\epsilon)(\log\log\log x)^2\right) \tag{1}$$

for $C = 0.8178\ldots$.

In Section 3 we show that the bound (1) is the best we can obtain given the currently known major constructions for Hadamard matrices. This is perhaps surprising, since (1) is obtained by taking Kronecker products of Paley Hadamard matrices only. So one might expect that the bound could be improved by incorporating the many other known constructions for Hadamard matrices.

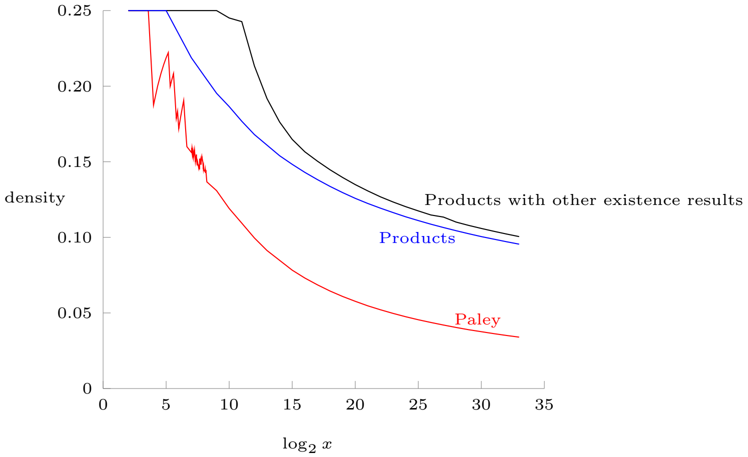

Figure 1: Density of Hadamard orders from different constructions

Figure 1 shows plots of three lower bounds for $S(x)$. These are obtained by taking into account the orders of various classes of known Hadamard matrices. The weakest bound is obtained using Paley orders $2^\alpha(p+1)$, where $\alpha \geq 1$ if $p \equiv 1 \pmod 4$, and $\alpha \geq 0$ otherwise. The second bound takes products of these orders, and the best bound adds products of the known Hadamard matrices of order up to 10000, and the constructions described in Section 3. We show in that section that these two bounds are in fact asymptotically equal. Indeed the impact of the table of known orders less than 10000 seems to fade quite rapidly.

The Paley bound is weaker than the others, but is still stronger than the bounds given by the asymptotic existence results proved by Seberry and

Craigen and Kharaghani. Interestingly, Figure 1 shows that the Hadamard Conjecture is decided in the affirmative for about one half of the orders $n \equiv 0 \pmod 4$ of size about one billion. So at least for “small” orders we are doing quite well.

We think that the notion of density has a wider applicability in the context of design theory. Typically, design theorists gauge the progress on a problem by creating tables of known orders and undecided cases. For example, we now know that Hadamard’s Conjecture holds for nearly all orders less than 10 000. However, many of the known constructions arise from algebraic or computer constructions which may fail to cover all cases as the upper bound on the orders to be covered is increased. So success for small orders may be misleading.

The existence question for Williamson matrices is a good example of this phenomenom. Williamson matrices of order t can be used to construct a Williamson-type Hadamard matrix of order $4t$. In [9] the authors obtain by computer search Williamson matrices of order 23, and thereby construct a Williamson-type Hadamard matrix of order 92. Flushed with this success, they then suggest that Williamson type Hadamard matrices exist for every order divisible by four. Indeed, subsequent computer searches confirmed that Williamson matrices exist for all odd orders up to and including 33. However, in [5] it was shown that no Williamson matrices exist for order 35, and since then additional computer searches [10] showed nonexistence for several more orders, so that now the question of how common Williamson matrices are for larger orders is quite unclear.

Therefore, there is a need for some other more global measure of the status of a design-theoretic existence question. Since such existence questions usually involve two infinite sets: one consisting of the decided orders and another consisting of the undecided orders, we think that the discrepancy between the sizes of the set of undecided orders and the set of decided orders provides a precise mathematical measure of the progress made on such existence questions.

The rest of this paper is divided into three parts. Section 2 derives a series of lower bounds for $S(x)$. These bounds are all implied by Paley’s construction for Hadamard matrices. Section 2 also contains a proof of Theorem 1.3. Section 3 contains a proof that taking into account the other major constructions for Hadamard matrices does not lead to a larger lower bound for $S(x)$. The proof uses the idea of a monoid of natural numbers: i.e., a set of natural numbers containing 1 which is closed under multiplication.

The final part of the paper is a technical appendix which proves two results concerning monoids which are needed in Section 3. The first part of the appendix contains elementary proofs of the monoid theorems, and the second part of the appendix gives proofs using results about generating functions.

2 Lower Bounds for $S(x)$ Using Paley Hadamard Matrices

In this section, we use Paley's family of Hadamard matrices to obtain three increasingly stronger lower bounds for $S(x)$.

2.1 A Simple Lower Bound

Theorem 2.1 (Paley). *For any prime q, there is a Hadamard matrix of order n, where*

$$n = \begin{cases} q+1, & \text{if } q \equiv 3 \pmod 4, \\ 2(q+1), & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

Dirichlet's Theorem on primes in arithmetic progressions implies the following corollary:

Corollary 2.2.

$$S(x) \geq \left(\frac{3}{4} + o(1) \right) \frac{x}{\log x}.$$

Proof. One has $(1/2 + o(1))x/\log x$ orders from primes $\equiv 3 \bmod 4$ up to x, and $(1/4 + o(1))x/\log x$ from primes $\equiv 1 \bmod 4$ up to $x/2$. An order m is in both sets if $p = m - 1$ and $q = m/2 - 1$ are both prime. Since $2q + 1 = p$, these are Sophie Germain primes. Brun's sieve may be used to show that the number of Sophie Germain primes up to x is $O(x/(\log x)^2)$ (see [12]), so this overlap does not affect the density. □

2.2 An Improvement

A Hadamard matrix of order n can be used to construct one of order $2n$, so we have ones of order $2^t(q + 1)$ for $t \geq 1$ for all primes q. This improves the bound in Corollary 2.2:

Corollary 2.3.

$$S(x) \geq \left(\frac{3}{2} + o(1)\right) \frac{x}{\log x}.$$

Proof. We use the following slightly stronger version of the Prime Number Theorem:

$$\pi(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right).$$

As before, we have $(1/2 + o(1))x/\log x$ orders from the primes $\equiv 3 \bmod 4$ up to x.

Now consider the set of orders $2(p+1)$ for all $p < x/2$. The number of these orders is

$$\begin{aligned} \pi(x/2) &= \frac{x/2}{\log(x/2)} + \frac{x/2}{\log^2(x/2)} + O\left(\frac{x}{\log^3 x}\right) \\ &= \frac{x}{2\log x} + \left(\frac{1+\log 2}{2}\right) \frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right). \end{aligned}$$

Similarly, from all primes $p < x/2^k$ for $k < \log x$ we get

$$\begin{aligned} \pi(x/2^k) &= \frac{x/2^k}{\log(x/2^k)} + \frac{x/2^k}{\log^2(x/2^k)} + O\left(\frac{x}{\log^3 x}\right) \\ &= \frac{x}{2^k \log x} + \frac{1+k\log 2}{2^k} \frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right). \end{aligned}$$

orders of the form $2^k(p+1)$. Summing these terms, the coefficient of $x/\log x$ converges to $3/2$, and the coefficient of $x/\log^2 x$ also converges.

The final step is to ensure that the intersection of the sets is small: the number of orders m with $p = m/2^r - 1$ and $q = m/2^s - 1$ for primes p and q is $o(x/\log x)$. As for Corollary 2.2, the number of such orders for any individual r and s is $O(x/\log^2 x)$ using Brun's sieve. Furthermore, we need only consider $r, s < 2\log\log x$, since the number of primes p up to $m/2^{2\log\log x}$ is $O(x/\log^3 x)$, and so the number of orders $m = 2^r(p+1)$ is $O(x/\log^2 x)$. Combining these results, the number of orders in more than one set is $o(x/\log x)$. □

2.3 Proof of Theorem 1.3: Further Improvements Via Products of Paley Matrices

Given Hadamard matrices of orders a and b, it is easy to construct a Hadamard matrix of order ab, but [1] and [4] show that we can do better:

Theorem 2.4. *If Hadamard matrices of order $4a$ and $4b$ exist, then there is a Hadamard matrix of order $8ab$.*

Theorem 2.5. *If Hadamard matrices of order $4a$, $4b$, $4c$ and $4d$, exist, then there is a Hadamard matrix of order $16abcd$.*

We want to show that applying these theorems to Paley Hadamard matrices will give us a greater density. An improvement follows immediately from a result of Erdős. He showed that the number of different values of $m = (p+1)(q+1)$ up to x, for p and q prime, is $(1+o(1))\frac{x(\log\log x)}{\log x}$. Thus

$$S(x) \geq (1+o(1))\frac{x}{\log x}(\log\log x)\,.$$

Thus we have an immediate improvement by taking into account Theorems 2.4 and 2.5.

A further improvement follows from theory that has been developed to analyze the distribution of values of the Euler totient function. The new bound (which is somewhat complicated) will imply that, for any $\alpha > 0$,

$$S(x) \geq (1+o(1))\frac{x}{\log x}(\log\log x)^{\alpha}\,.$$

Recall that the Euler totient function $\varphi(n)$ is the number of positive integers less than n which are relatively prime to n. This is a multiplicative function with value at prime powers:

$$\varphi(p^a) = p^{a-1}(p-1)\,.$$

Let $V(x)$ be the number of distinct values of Euler's φ-function less than x. The study of the growth of $V(x)$ has a long history. In 1929 Pillai [11] showed

$$V(x) \ll \frac{x}{\log^{\log 2/e} x}\,.$$

In 1935 Erdős [6] improved this to

$$V(x) \ll \frac{x}{\log^{1+o(1)} x}\,.$$

The $o(1)$ was subsequently made more precise by Erdős and Hall, Pomerance, Maier and Pomerance, and finally Ford [8], who showed

$$\begin{aligned} V(x) \quad &= \quad \frac{x}{\log x} \exp\big(C(\log\log\log x - \log\log\log\log x)^2 \\ &\qquad +D\log\log\log x - (D+1/2-2C)\log\log\log\log x + O(1)\big)\,, \end{aligned} \tag{2}$$

where $C = 0.8178\ldots$ and $D = 2.1769\ldots$.

Ford proved that this bound applies to *any* multiplicative function f satisfying two conditions:

$$\{f(p) - p : p \text{ prime}\} \text{ is a finite set not containing } 0 \tag{3}$$

$$\sum_{h\geq 16 \ squareful} \frac{\epsilon(h)}{f(h)} \ll 1,\ \epsilon(h) = \exp(\log\log h(\log\log\log h)^{20}). \tag{4}$$

Note that $n \in \mathbb{N}$ is squareful if, for all primes p, $p|n$ implies $p^2|n$.

Proof. (Proof of Theorem 1.3) We now use Ford's general theory to prove Theorem 1.3. We take $f(p^k) = f_2(p^k) = (p+1)^k$. Then condition (3) holds. Moreover, $f_2(x) > \varphi(x)$; so (4) holds for $f = f_2$, since it holds for $f = \varphi$. Thus Ford's result implies, that the set of integers up to x of the form

$$(p_1+1)^{\alpha_1}(p_2+1)^{\alpha_2}\cdots(p_k+1)^{\alpha_k} \tag{5}$$

has density of the same form as the righthand side of (2). This expression is only determined up to the "$O(1)$" term in the exponent. Nevertheless, since (by Theorems 2.1 and 2.4) there are Hadamard matrices for all orders $2t$, where t has the form (5), $S(x)$ is bounded below by a function of the form on the righthand side of (2). Theorem 1.3 now follows. □

One issue, involving powers of two, remains to be discussed. For each prime $p_i \equiv 1 \bmod 4$ in (5), the order of the Paley matrix is $2(p_i+1)$, not $p_i + 1$. However, this is offset by Theorems 2.4 and 2.5, which show that if $\alpha_1 + \alpha_2 + \cdots + \alpha_k = A$, we may divide (5) by a factor of two raised to the power:

$$4\lfloor(A-1)/3\rfloor + ((A-1) \bmod 3).$$

Potentially this could give us an increase in our lower bound for $S(x)$, say if we had a large number of integers in $\mathcal{S}(x)$ with $\sum \alpha_i \geq \log\log x$. However, Ford's Theorem 10 (and its generalization to other multiplicative functions) shows that almost all integers in $\mathcal{S}(x)$ have

$$\sum_i \alpha_i = 2C(1 + o(1)) \log\log\log x$$

as $x \longrightarrow \infty$. Therefore the savings from dividing out by powers of two does not affect the main term in Theorem 1.3.

3 The Impact of Other Constructions

In this section, we show that our best lower bound for $S(x)$ cannot be improved by taking into account other large classes of known Hadamard matrices. In order to do so, we introduce the following key idea:

Definition 3.1. A subset $\mathcal{A}$ of $\mathbb{N}$ is called a (multiplicative) monoid if

- $1 \in \mathcal{A}$, and
- $a, b \in \mathcal{A}$ implies $ab \in \mathcal{A}$.

The set $\mathcal{G}$ generates a monoid $\mathcal{M}$ if every element in $\mathcal{M}$ is a product of elements in $\mathcal{G}$.

Notice that if $\mathcal{A}$ and $\mathcal{B}$ are monoids, then the product set $\mathcal{A}\mathcal{B} = \{ab : a \in \mathcal{A},\ b \in \mathcal{B}\}$ is a monoid.

Our interest in monoids stems from the observation that the set of known Hadamard orders is closed under multiplication: i.e., the product $n_1 n_2$ of two known Hadamard orders n_1, n_2 is also a known Hadamard order. Indeed, any construction for Hadamard matrices generates a monoid of known Hadamard orders via the Kronecker product and the product results Theorems 2.4 and 2.5.

Our overall plan in this section will be to determine the size of the monoid generated by each major known construction, and then to determine the size of the product of these monoids.

The following theorem allows us to determine the size of the products of the monoids encountered in this section. It is perhaps surprising that taking finite products of monoids often does not give a significantly larger monoid.

Theorem 3.2. *Suppose that $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C} = \mathcal{A}\mathcal{B}$ are monoids such that $A(x) = O(x^\alpha)$ and $B(x) = \Omega(x^\beta)$, where $0 < \alpha < \beta < 1$. Then $C(x) = O(B(x))$.*

So up to a constant factor, the product monoid has the same size as the larger of the two monoids.

We will also need a result which bounds the size of a monoid in terms of the size of its generating sets. The next theorem shows that if a monoid has a fairly small generating set, then the monoid itself is not much larger.

Theorem 3.3. *Let $\mathcal{G}$ be a subset of $\mathbb{N}$ such that $G(x) = O(x^\alpha)$, for some $\alpha \in (0,1)$. Let $\mathcal{M}$ be the monoid generated by $\mathcal{G}$. Then $M(x) = O(x^{\alpha+\epsilon})$ for all $\epsilon > 0$.*

Notice that a monoid has a unique minimal generating set: namely, the set of elements in the monoid which are not the product of strictly smaller elements of the monoid. The theorem of course applies to any generating set. See the Appendix for proofs of Theorems 3.2 and 3.3.

The following families are given in the survey article [3]:

1. Hadamard matrices exist for every order ≤ 662. Tables of known orders $2^t g$ are given for odd $g < 9999$.

2. A Hadamard matrix of order $2^t g$ for odd g exists for
$$t \geq 6 \left\lfloor \frac{\log_2 \frac{g-1}{2}}{16} \right\rfloor + 2.$$

3. For g odd with k nonzero digits in its binary expansion, there is a Hadamard matrix of order $2^t g$ when
   (a) $g \equiv 1 \pmod 4$ and $t \geq 2k$,
   (b) $g \equiv 3 \pmod 4$ and $t \geq 2k - 1$.

4. For q a prime power, $q \not\equiv 7 \pmod 8$ a Hadamard matrix of order $4q^2$ exists.

5. For q odd, a Hadamard matrix of order $4q^4$ exists.

6. If $n-1$ and $n+1$ are both odd prime powers, then there exists a Hadamard matrix of order n^2.

We also note the large class of cocyclic[1] Hadamard matrices:

7 Let $p_1, p_2, \ldots, p_r \equiv 1 \pmod 4$ and let $q_1, q_2, \ldots, q_s \equiv 3 \pmod 4$ be prime powers. Then, for all $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_s \geq 0$, there is a cocylic Hadamard matrix of order

$$\prod_{i=1}^{r} 2p_i^{\alpha_i}(p_i + 1) \prod_{i=1}^{s} q_i^{\beta_i}(q_i + 1)\,.$$

We first observe that the orders in the last class form a monoid $\mathcal{M}_7$ whose size has the same form as $V(x)$. To see this, we define $f_3(p^k) = p^{k-1}(p + 1)$, and then apply Ford's theorem. Notice that $f_3(x) > \varphi(x)$; so condition (4) holds for f_3 since it holds for the totient function φ.

Notice also that, if $\mathcal{M}'_7$ includes all the orders obtained by applying Theorems 2.4 and 2.5 to the orders listed under item 7, then $\mathcal{M}'_7$ contains all the orders identified in the previous section. Moreover, the argument at the end of Section 2 implies that $\mathcal{M}_7$ and $\mathcal{M}'_7$ have about the same size.

We now show that the Hadamard orders given by constructions 1–6 in combination generate a monoid whose size is quite small.

Theorem 3.4. *The monoid $\mathcal{M}$ generated by all the orders given by constructions 1–6 has size $O(x^{8/11+\epsilon})$, where $\epsilon > 0$ may be taken as close to zero as one pleases.*

Proof. We consider the constructions 1–6 listed above in order:

1. The first construction generates a monoid $\mathcal{M}_1$ which has a finite number of generators. So $\mathcal{M}_1 \cap [1, x]$ has size $O((\log x)^a)$, where a is the number of generators.

2. Let $\mathcal{M}_2$ be the monoid generated by the set $\mathcal{G}_2$ of orders given by the second construction. Then $\mathcal{M}_2$ is not much smaller than the set

$$\{2^t g \mid \text{where } g \text{ is odd and } t \geq \epsilon \log_2 g\}\,,$$

where $\epsilon = 3/8$. The number of elements in this set is about equal to

$$\sum_{g^{1+\epsilon} \ odd \ \leq x} \log_2(x/g^{1+\epsilon}) = O(x^{\frac{1}{1+\epsilon}} \log x)\,.$$

[1] Cocyclic Hadamard matrices correspond to certain relative difference sets.

3. To assess the size of the monoid $\mathcal{M}_3$ given by this construction, we apply Theorem 3.3.

   Let $\mathcal{G}_3$ be the set of orders $2^t g$ satisfying parts (a) and (b) of item 3 above. Then $\mathcal{G}_3$ generates $\mathcal{M}_3$. We now estimate the size of $\mathcal{G}_3 \cap [1, x]$. Put $n = \lceil \log_2 x \rceil$, and suppose $2^t g \in \mathcal{G}_3 \cap [1, x]$. If $g \equiv 1 \pmod 4$ has has exactly k digits equal to 1, then the bottom $2k$ digits of the binary expansion of $2^t g$ must be zero, and the remaining $n - 2k$ digits must contain exactly k 1s. This gives at most $\binom{n-2k}{k}$ possibilities. If $g \equiv 3 \pmod 4$ has exactly k digits equal to 1, then the bottom $2k - 1$ digits of the binary expansion of $2^t g$ must be zero, and the remaining $n-2k+1$ digits must contain exactly k 1s. This gives at most $\binom{n-2k+1}{k}$ possibilities. So

   $$G_3(x) \leq \sum_k \binom{n-2k+1}{k} + \binom{n-2k}{k}.$$

   There are at most n summands, and the largest of these occurs when $k \approx n/4$. So $G_3(x) = O(x^{\frac{1}{2}+\epsilon})$ for any $\epsilon > 0$. Theorem 3.3 now implies that $M_3(x) = O(x^{\frac{1}{2}+\epsilon})$ for any $\epsilon > 0$.

4. Constructions 4, 5 and 6 all give orders lying in the monoid $\mathcal{M}_4$ of square orders. So the monoid generated by these orders has size $O(x^{1/2})$.

The monoids $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$ and $\mathcal{M}_4$ all have size $O(x^\delta)$ where $\delta > 8/11$ may be taken as close to $8/11$ as one pleases. So Theorem 3.3 implies the result. □

From Theorem 3.4 and Theorem 3.2 we see that constructions 1–7 do not increase the asymptotic bound for $S(x)$:

Theorem 3.5. *The monoid $\mathcal{M}_0$ generated by constructions 1–7 has size*

$$\frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right)$$

for $C = 0.8178\ldots$.

Acknowledgements

The authors would like to thank Carl Pomerance for directing them to the literature on the distribution of Euler's function.

References

[1] S. S. Agayan. *Hadamard Matrices and their Applications*. Springer-Verlag, 1985.

[2] D. J. Bernstein. Arbitrarily tight bounds on the distribution of smooth integers. In M. A. Bennett et al., editor, *Number theory for the millennium I*, pages 49–66. A K Peters, 2002.

[3] R. Craigen and H. Kharaghani. Hadamard matrices and Hadamard designs. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, pages 273–280. CRC Press, second edition, 2007.

[4] R. Craigen, J. Seberry, and X. Zhang. Product of four hadamard matrices. *JCT A*, 59:318–320, 1992.

[5] D. Z. Doković. Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete Math.*, 115:267–271, 1993.

[6] P. Erdős. On the normal number of prime factors of $p - 1$ and some related problems concerning Euler's ϕ-function. *Quart. J. Math. (Oxford)*, 6:205–213, 1935.

[7] P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge Press, 2009.

[8] K. Ford. The distribution of totients. *The Ramanujan Journal*, 2:67–151, 1998.

[9] S.W. Golomb and L.D. Baumert. The search for Hadamard matrices. *Amer. Math Monthly*, 70:12–17, 1963.

[10] W.H. Holzmann, H. Kharaghani, and B. Tayfeh-Resaie. Williamson matrices up to order 59. *Des. Codes Cryptogr.*, 46:343–352, 2008.

[11] S. S. Pillai. On some functions connected with $\varphi(n)$. *Bull. Amer. Math. Soc.*, 35:832–836, 1929.

[12] P. Ribenboim. *The New Book of Prime Number Records.* Springer-Verlag, 1995.

A Monoids and Sets of Natural Numbers

In this appendix, we prove two theorems showing that taking products of sets does not greatly increase asymptotic density. We give two sets of proofs; one elementary and self-contained, and the other shorter but depending on results on generating functions.

In this paper, we use some standard notation to discuss the growth of the counting function of a set: Let $f : \mathbb{N} \to \mathbb{R}$ be a function. Then

- "$A(x) = O(f(x))$" means that there is a constant $C > 0$ and $x_0 \in \mathbb{N}$ such that $A(x) < Cf(x)$ for all $x \geq x_0$,
- "$A(x) = \Omega(f(x))$" means that there is a constant $C > 0$ and $x_0 \in \mathbb{N}$ such that $A(x) > Cf(x)$ for all $x \geq x_0$.
- "$A(x) = \Theta(f(x))$" means that there are constants $c_1 > c_2 > 0$ and $x_0 \in \mathbb{N}$ such that $c_1 f(x) \geq A(x) \geq c_2 f(x)$ for all $x \geq x_0$.
- "$A(x) = o(f(x))$" means that for any constant $C > 0$ there is some $x_0 \in \mathbb{N}$ such that $A(x) < Cf(x)$ for all $x \geq x_0$.

A.1 Elementary Proofs

For any subset $\mathcal{A}$ of $\mathbb{N}$ and any $x \in \mathbb{N}$, let

$$a(x) = |\mathcal{A} \cap (x/2, x]| \qquad \text{and} \qquad \bar{a}(x) = |\mathcal{A} \cap [x/2, x]| \,.$$

Lemma A.1. *Let $\mathcal{A}, \mathcal{B}$ and $\mathcal{C} = \mathcal{A}\mathcal{B}$ be subsets of $\mathbb{N}$ which are monoids. Then, for all $x \in \mathbb{N}$,*

$$\frac{c(x)}{b(x)} \leq \sum_{k=1}^{\lceil \log_2 x \rceil} \frac{(b(x/2^{k-1}) + b(x/2^k))\bar{a}(2^k)}{b(x)} \,. \tag{6}$$

Moreover, if the righthand side is bounded by a constant c_1, say, for all $x \in \mathbb{N}$, then $C(x) = \Theta(B(x))$.

Proof. Since every element of $\mathcal{C} \cap (x/2, x]$ can be written in the form ab, where, for some $k \in \{1, 2, \ldots, \lceil \log_2 x \rceil\}$, $a \in \mathcal{A} \cap [2^{k-1}, 2^k]$ and $b \in \mathcal{B} \cap (x/2^{k+1}, x/2^{k-1}]$, we have

$$c(x) \le \sum_{k=1}^{\lceil \log_2 x \rceil} (b(x/2^{k-1}) + b(x/2^k))\bar{a}(2^k)\,.$$

Dividing through by $b(x)$ then gives (6). We now prove the second part of the lemma. By hypothesis, we have

$$c(x) \le b(x) \left\{ \sum_{k=1}^{\lceil \log_2 x \rceil} \frac{(b(x/2^{k-1}) + b(x/2^k))\bar{a}(2^k)}{b(x)} \right\} \le c_1 b(x)\,.$$

Now we have the following partition

$$\mathcal{C} \cap [1, x] = \bigcup_{k=1}^{\lceil \log_2 x \rceil} \mathcal{C} \cap (x/2^k, x/2^{k-1}]$$

for $\mathcal{C} \cap [1, x]$ and a similar partition for $\mathcal{B} \cap [1, x]$. So

$$C(x) = \sum_{k=1}^{\lceil \log_2 x \rceil} c(x/2^{k-1}) \le c_1 \sum_{k=1}^{\lceil \log_2 x \rceil} b(x/2^{k-1}) = c_1 B(x)\,.$$

Since $\mathcal{B} \subset \mathcal{C}$, we then have $B(x) \le C(x) \le c_1 B(x)$. This completes the proof of the second part of the lemma. □

Proof of Theorem 3.2: For some constants $c_1, c_2 > 0$,

$$b(x) = B(x) - B(\lfloor x/2 \rfloor) \ge c_1 x^\beta - c_2 \left(\frac{x}{2}\right)^\beta = \left(\frac{x}{2}\right)^\beta (2^\beta c_1 - c_2)$$

Now

$$\begin{aligned} \sum_{k=1}^{\lceil \log_2 x \rceil} \frac{(b(x/2^{k-1}) + b(x/2^k))\bar{a}(2^k)}{b(x)} &\le \sum_{k=1}^{\lceil \log_2 x \rceil} \frac{B(x/2^{k-1})A(2^k)}{b(x)} \\ &\le c_3 \sum_{k=1}^{\lceil \log_2 x \rceil} \left(\frac{x}{2^{k-1}}\right)^\beta 2^{k\alpha} \left(\frac{2}{x}\right)^\beta \\ &\le c_4 \sum_{k=1}^{\lceil \log_2 x \rceil} 2^{k(\alpha-\beta)}\,, \end{aligned}$$

which is bounded since $\alpha < \beta$. So Lemma A.1 implies that $C(x) = \Theta(B(x))$.

We now prove Theorem 3.3, that the size of a monoid is at most slightly bigger than its generating set:

Proof of Theorem 3.3: Fix $\epsilon > 0$. We prove $M(x) = O(x^{\alpha+\epsilon})$. Put $\alpha_0 = \alpha + \epsilon/2$. Let x_0 be such that $G(x) \leq \frac{1}{2}x^{\alpha_0}$ for all $x \geq x_0$. Let $\mathcal{G}_0 = \mathcal{G} \cap [1, x_0)$, and let $\mathcal{G}_1 = \mathcal{G} \cap [x_0, \infty)$. Let $\mathcal{M}_0$ be the monoid generated by $\mathcal{G}_0$, and let $\mathcal{M}_1$ be the monoid generated by $\mathcal{G}_1$. Then the following statements hold:

(A) $G_1(x) \leq \frac{1}{2}(x^{\alpha_0})$,

(B) $M_0(x) = O((\log x)^{|\mathcal{G}_0|})$,

(C) $\mathcal{M} = \mathcal{M}_0\mathcal{M}_1$,

(D) $M(x) \leq M_0(x)M_1(x) = O((\log x)^{|\mathcal{G}_0|}M_1(x))$.

So, noting item (D), in order to prove that $M(x) = O(x^{\alpha+\epsilon})$, it is sufficient to prove that $M_1(x) = O(x^{\alpha_1})$, for all $\alpha_1 \in (\alpha_0, \alpha + \epsilon)$.

Fix $\alpha_1 \in (\alpha_0, \alpha + \epsilon)$. We prove $M_1(x) = O(x^{\alpha_1})$. Let $n = \lceil \log_2 x \rceil$. Any element y of $\mathcal{M}_1 \cap [1, x]$ corresponds to a partition of n as follows: Suppose $y = y_1 y_2 \ldots y_r$ where $y_1 \leq y_2 \leq \cdots \leq y_r$ are elements of $\mathcal{G}_1$. Put $a_i = \lfloor \log_2 y_i \rfloor$. Then $a_1 + a_2 + \ldots a_r = m \leq n$, and $0 \leq a_1 \leq a_2 \leq \cdots \leq a_r$. Thus replacing a_r with $a'_r = a_r + n - m$, we see that any product $y = y_1 y_2 \ldots y_r \in \mathcal{M}_1 \cap [1, x]$ of r elements y_i of $\mathcal{G}_1$ maps to a partition of n into at most r pieces. The number of such y sequences $y_1, y_2, \ldots, y_r$ with $\lfloor \log_2 y_i \rfloor = a_i$ is at most

$$G_1(2^{a_1+1})G_1(2^{a_2+1}) \ldots G_1(2^{a_r+1}) \leq 2^{a_1\alpha_0}2^{a_2\alpha_0} \ldots 2^{a_r\alpha_0} \leq 2^{n\alpha_0}\,.$$

Now Hardy and Ramanujan showed that the number $p(n)$ of partitions of n is asymptotic to

$$\exp(\pi\sqrt{2n/3})/4n\sqrt{3} = O(x^{\delta})\,,$$

for all $\delta > 0$. So, choosing $\delta = \alpha_1 - \alpha_0$, we have

$$M_1(x) \leq p(n)2^{\lceil \log_2 x \rceil \alpha_0} = O(x^{\alpha_0+\alpha_0}) = O(x^{\alpha_1})\,.$$

A.2 Proofs using Generating Functions

We will use generating functions to show that these constructions do not increase the density of known Hadamard orders. Since we are interested in the properties of products of sets $\mathcal{C} = \mathcal{A}\mathcal{B}$, functions of the form

$$\sum_{n \in \mathcal{A}} z^{\log_2 n}$$

are useful, since multiplying elements corresponds to adding the powers in terms of the series. In the context of smooth numbers, Bernstein [2] estimated such functions by looking at

$$a(z) = \sum_{k \geq 0} a_k z^k := \sum_{n \in \mathcal{A}} z^{\lfloor \log_2 n \rfloor}.$$

These series have many fewer terms, and so are easier to analyze. Note that $a_k = A(2^k) - A(2^{k-1})$ is the number of k-bit elements of $\mathcal{A}$. We will prove results about a_k, i.e. $A(x)$ for x a power of two, but since $A(x)$ is monotone increasing, and all the coefficients of the generating function are nonnegative, this will suffice.

Lemma A.2. *Let $\mathcal{C}$ be the set of products of elements of sets $\mathcal{A}$ and $\mathcal{B}$ with series $a(z)$ and $b(z)$. Then*

$$c(z) \leq a(z) \frac{b(z)}{1-z}.$$

Proof. The coefficient of z^n in $a(z)\frac{b(z)}{1-z} = a(z)b(z)(1 + z + z^2 \cdots)$ is

$$\sum_{k=0}^{n} a_k B(2^{n-k}).$$

Any n-bit element of $\mathcal{C}$ can be written as a product of a k-bit element of $\mathcal{A}$ and an element of $\mathcal{B}$ of at most $n-k$ bits. □

We may use the analytic properties of series like this to bound the size of the corresponding counting function. Flajolet and Sedgewick [7] give a wealth of such results. Their Theorem IV.7 relates the growth rate of power series coefficients to singularities of the corresponding function:

Theorem A.3. *If $f(z) = \sum f_n z^n$ has positive coefficients and is analytic at* 0 *and*

$$R = \sup\{r \geq 0 | f \text{ is analytic at all points of } 0 \leq z < r\}$$

then $\limsup |f_n|^{1/n} = (1/R)$.

From Corollary 2.2 we have $s_k = \Theta(2^{(1-\epsilon)k})$ for any $\epsilon > 0$, so by the ratio test the radius of convergence of $s(z)$ is $1/2$. The coefficients of generating functions for the other monoids have smaller growth, and so a larger radius of convergence. Theorem VI.12 of [7] shows that the size of the product set $\mathcal{AB} = \{ab | a \in \mathcal{A}, b \in \mathcal{B}\}$ of two sets with different growth rates is a constant times the size of the larger set, proving Theorem 3.2:

Theorem A.4. *Suppose $a(z) = \sum a_n z^n$ and $b(z) = \sum b_n z^n$ are power series with radii of convergence $\alpha > \beta \geq 0$, respectively. Suppose b_{n-1}/b_n approaches a limit b as $n \longrightarrow \infty$. If $a(b) \neq 0$, then $c_n \sim a(b) b_n$, where $\sum c_n z^n = a(z)b(z)$.*

Finally consider the monoid generated by a set $\mathcal{A}$. The generating function for the monoid will be

$$\operatorname{Exp}(a(z)) := \exp\left(a(z) + \frac{1}{2}a(z^2) + \frac{1}{3}a(z^3) + \cdots\right).$$

This function has the same radius of convergence as $a(z)$ (see Section IV.4 of [7]), giving Theorem 3.3.